Qwest
607 14th Street, NW, Suite 950
Washington, DC 20005
Phone 303-383-6651
Facsimile 303-896-1107

Kathryn Marie Krause
Associate General Counsel

March 1, 2010

FILED VIA ECFS

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to the Federal Communications Commission's *Report and Order*,[1] Qwest hereby files its Annual 47 C.F.R. § 64.2009(e) CPNI Certification.

Please contact me at the above-listed information if you have any questions.

/s/ Kathryn Marie Krause

cc: Best Copy and Printing, Inc. (fcc@bcpiweb.com)

---

[1] *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007). *Also see*, Public Notice, DA 10-91 (Jan. 15, 2010).

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket No. 06-36

Annual 64.2009(e) Customer Proprietary Network Information (CPNI) Certification for 2010, covering the prior calendar year 2009.

Date filed: March 1, 2010

Name of companies covered by this certification:

Form 499 Filer ID: 808440 Qwest Corporation
814711 Malheur Home Telephone Company (merged into Qwest Corporation 12.31.2009)
807684 El Paso County Telephone Company
808439 Qwest Wireless, LLC
808882 Qwest Communications Company, LLC
822734 Qwest LD Corp.

Name of signatory: Alwin Roberts

Title of signatory: Senior Vice President and General Manager–Mass Markets

I, Alwin Roberts, am an officer of Qwest Corporation (a local exchange carrier). Acting as an agent of that company, and on behalf of the other companies identified above (collectively Qwest), I certify that I have personal knowledge that these companies have established operating procedures that are adequate to ensure compliance with the Federal Communications Commission (FCC) CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq*. My personal knowledge is based, in part, on the personal knowledge of those persons who represent to me that their organizations have procedures in place adequate to ensure compliance with the FCC's CPNI rules.

Attached to this certification is an accompanying statement describing how the various companies have established operating procedures that are adequate to ensure compliance (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) with the requirements set forth in section 64.2001 *et seq.* of the FCC's rules.

Actions Against Data Brokers. None of the Qwest companies identified above took action in 2009 against data brokers either in courts or before regulatory bodies.

Customer Complaints. ***See*** **Exhibit 2.** The Qwest companies identified above received 7 customer complaints, one of which was deemed unfounded. Among the 7 complaints, 4 involved allegations of improper access to **online** information; 2 related to unauthorized access to a customer's account; and 1 involved allegations of improper access and disclosure of CPNI, by a Qwest employee, to individuals not authorized to receive it.

Acting on behalf of the above-identified companies, they represent and warrant that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The companies also acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject them to enforcement action.

Signed /s/ Alwin Roberts
[Electronic Signature]

Attachments: Accompanying Statement explaining CPNI procedures, Exhibit 1
Summary of Customer Complaints, Exhibit 2

EXHIBIT 1 TO COMPLIANCE CERTIFICATE
Qwest Statement of Operating Procedures

Below, Qwest describes its operating procedures to ensure compliance with the Federal Communications Commission (FCC) Customer Proprietary Network Information (CPNI) rules set forth in 47 C.F.R., Subpart U:

1. Alwin Roberts, Senior Vice President and General Manager in Mass Markets is Qwest's CPNI Certifying Officer. Once a year, Qwest utilizes a certification process in which the managers of those business units that might use CPNI for sales or marketing certify to Mr. Roberts that, based on their personal knowledge, their business and market units have practices and procedures in place to ensure compliance with the FCC's CPNI rules.

2. Qwest also takes advantage of the expertise and experience of a variety of its other (non-sales) organizational units and personnel in addressing privacy and CPNI issues. Qwest has a Chief Privacy Officer (CPO), within the Risk Management organization, whose duties include advice and counsel on a variety of privacy issues. Within that Risk Management organization there is also an Information Security and Technology group, and technical CPNI issues are vetted with it. Still within that organization, Qwest has a dedicated CPNI Compliance Manager with more than a decade of experience in addressing and counseling on the proper uses of CPNI. That Compliance Manager, along with other Qwest Risk Management employees, including the CPO and the Information Security and Technology group, is responsible for assisting Qwest business units on a host of issues, including product development, training, discipline and supervision of marketing campaigns. Finally, all of the Qwest employees referenced above interact with senior Qwest legal counsel on CPNI matters that require legal analysis or advice. That counsel has been involved in CPNI issues for over 25 years. Qwest is confident that this cooperative and collaborative cross-discipline approach to CPNI issues creates an atmosphere and structure that frame and support operating procedures adequate to ensure compliance with the FCC's CPNI rules.

3. In order to ensure that CPNI issues are resolved uniformly across the business and in a timely manner, the CPNI Compliance Manager hosts bi-weekly (and if necessary weekly) CPNI conference calls which are attended by senior CPNI legal counsel. When appropriate, members of the business units, Qwest's CPO, or other Qwest attorneys will attend these calls. During these calls, CPNI issues are discussed, issues are raised, solutions are reached and/or action plans are established. In addition, the CPNI Certifying Officer is consulted or advised as necessary.

4. In addition to the management structure addressed above that is designed to appropriately address CPNI issues, all Qwest employees receive training on CPNI rules. Employees with direct sales, marketing and product responsibilities receive

more-detailed training on the proper use of CPNI than the employee base generally. This detailed training includes instructions on how to recognize and properly address CPNI issues during inbound sales calls, as well as instruction on outbound marketing campaigns, including how CPNI may and may not be used during such campaigns and what administrative records must be kept. Further, on an ongoing basis, targeted training is conducted as needed. Additionally, in those cases where agents act as branded-Qwest representatives, Qwest provides appropriate training and scripting.

5. Beyond its formal training, Qwest has created CPNI "methods," available for all its employees that are likely to access, use or disclose CPNI. Those methods address, for example, how Qwest employees should deal with CPNI in the context of a telephone conversation or in a Qwest sales outlet. For example, the methods advise that employees should not disclose call detail records absent special customer verification (*i.e.*, a password), *unless* the customer provides the employee with specific details about the call in question so that the employee is responding to the information given by the customer. Those methods also state that in-store employees should not release CPNI to customers unless the customer presents a valid photo ID. Qwest publishes its methods internally for easy access and consultation and uses those methods in face-to-face training sessions, as well.

6. Qwest does not allow its customers to use biographical or account information to access CPNI online. Customers not exempt from the rules (*i.e.*, certain business customers) must authenticate themselves using a Qwest-issued security code to establish an online username and password. Additionally, Qwest has procedures regarding notifying customers when passwords, a response to a back-up means of authentication for a lost or forgotten password, online account, or address of record are created or changed.

7. Qwest sales personnel are required to obtain supervisory approval for their outbound marketing campaigns. They are required to maintain a record of their campaigns that use CPNI, including such details as: a description of the campaign (including the proposed dates and campaign purpose), the CPNI that was used and the products or services intended to be offered. The records are maintained for a minimum of one year.

8. Qwest makes CPNI available to independent vendors for marketing purposes when they have proof of authorization from the customer. These vendors generally sell "packages" of products, including telecommunications and information services, and customer premises equipment (CPE).

9. Qwest's primary systems used for sales and marketing allow representatives to determine a customer's CPNI-approval status prior to the use of CPNI. Other than duration-of-the-call CPNI approval, Qwest uses opt-in approval mechanisms. A customer's CPNI approval can be changed by a customer at anytime by contacting Qwest.

10. Qwest engages in quality assurance programs that monitor calls for, among other things, compliance with the CPNI rules and correct customer authentication. That program provides feedback to managers for training purposes; and if appropriate, disciplinary action.

11. Qwest has documented disciplinary procedures regarding CPNI errors beyond its quality assurance program. A potential violation of CPNI rules is investigated, and, where appropriate, disciplinary action is taken.

12. Qwest requires its employees to report the unauthorized access, use or disclosure of CPNI to a central point, *i.e.*, its general internal advice line, for further investigation. Customer complaints sometimes also come to Qwest's attention through that line.

13. Qwest takes reasonable measures to discover and protect against attempts to gain authorized access to CPNI. Qwest performs routine security evaluations and security assessments on Qwest systems, including those containing CPNI. Additionally, the Information Security and Technology group performs external penetration tests on Internet-facing web portals to ensure proper security is maintained. These activities further ensure that the necessary information-security safeguards are maintained with respect to CPNI and other customer information.

14. Qwest works with law enforcement regarding unauthorized access, use or disclosures of CPNI or other customer information when appropriate, even beyond the requirements of the FCC's rules. With respect to the reporting of CPNI "breaches" under the FCC-mandated process (*e.g.*, to the Department of Justice portal), Qwest has a single point-of-contact employee who does that reporting. That employee first reviews the allegations and, after investigation, if a breach warrants reporting, she does the reporting. A log of such reports is maintained and Qwest will be maintaining these records for at least two years.

EXHIBIT 2 TO COMPLIANCE CERTIFICATE
Qwest Statement of Customer Complaints

Qwest investigated each of the 7 complaints summarized below. Of them, all but one were deemed valid and reported to the Federal Bureau of Investigation (FBI) and United States Secret Service (USSS), through the portal established for improper CPNI disclosures.

Of the 7 customer complaints, 4 involved allegations of improper access to **online** information; 2 related to unauthorized access to a customer's account; and 1 involved allegations of improper access and disclosure of CPNI, by a Qwest employee, to individuals not authorized to receive it.

- 4 complaints were the result of isolated incidents in Qwest's systems, which have been resolved.

  March 10, 2009 - On or about March 10, 2009, Qwest received a customer complaint stating that the customer was able to view another customer's billing account information in one of Qwest's self service applications. Qwest investigated and resolved the programming issue which created this problem. Qwest has received no other complaints about it.

  April 21, 2009 - A Qwest employee reported that he was able to view his friend's residential account information online in Qwest's MyAccount platform. Qwest's investigation revealed the problem was caused by a coding change to Qwest's systems in the days immediately prior to these events. On learning of the problem, Qwest promptly resolved the issue and has received no other complaints about it.

  May 8, 2009 - On or about May 8, 2009, Qwest received **two** customer complaints stating that they were able to view another customer's billing account information in one of Qwest's self service applications for business customers being used by a small number of customers in a test phase. Qwest investigated and resolved the programming issue which created this problem. Qwest has received no other complaints about it.

- 2 complaints related to unauthorized access to a customer's account.

  January 19, 2009 - A concerned person informed Qwest that she received an order confirmation e-mail for an order on an account that was not hers. Qwest determined that she received the e-mail as the result of a simple typing error when the correct customer's e-mail was entered by the Qwest vendor who took the order. We have corrected our information on the proper customer's e-mail address and updated the security controls on that customer's account.

May 21, 2009 - A customer reported concern that an outside vendor had access to Qwest internal account records. Upon investigation, Qwest determined the concern was unfounded.

- 1 complaint involved an employee's improper release of CPNI.

  February 13, 2009 - A customer reported that her soon to be ex-son-in law (a Qwest employee), gained unauthorized access to the phone number and wireless account of her daughter (who was then the Qwest employee's wife.). Qwest's investigation revealed that the Qwest employee had accessed the account without authorization in July 2008. We disciplined the Qwest employee for unauthorized access to the customer's account in violation of Qwest's Code of Conduct and other policies.